



CVE-2002-1143

Published on: 04/03/2003 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:03 PM UTC

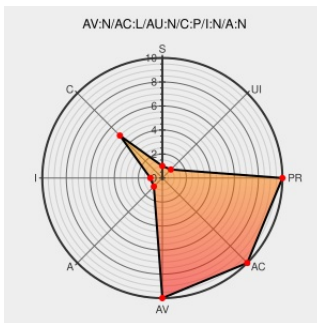
CVE-2002-1143

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Excel](#) from [Microsoft](#) contain the following vulnerability:

Microsoft Word and Excel allow remote attackers to steal sensitive information via certain field codes that insert the information when the document is returned to the attacker, as demonstrated in Word using (1) INCLUDETEXT or (2) INCLUDEPICTURE, aka "Flaw in Word Fields and Excel External Updates Could Lead to Information

Disclosure."

CVE-2002-1143 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Repository / Oval Repository	Third Party Advisory oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:202
Developer tools, technical documentation and coding examples Microsoft Docs	Patch Vendor Advisory www.microsoft.com text/html	CONFIRM www.microsoft.com/technet/treeview/default.asp?url=/Technet/security/topics/secword.asp
CERT/CC Vulnerability Note VU#899713	Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#899713

Microsoft Word / Excel INCLUDETEXT Document Sharing File Disclosure Vulnerability	Exploit Patch Third Party Advisory VDB Entry Vendor Advisory cve.report (archive) text/html	 BID 5586
Microsoft Security Bulletin MS02-059 - Moderate Microsoft Docs	docs.microsoft.com text/html	 MS MS02-059
'Security side-effects of Word fields' - MARC	Mailing List Third Party Advisory marc.info text/html	 BUGTRAQ 20020826 Security side-effects of Word fields
Microsoft Word INCLUDEPICTURE Document Sharing File Disclosure Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	 BID 5764
'More vulnerabilities (Re: Security side-effects of Word fields)' - MARC	Mailing List Third Party Advisory marc.info text/html	 BUGTRAQ 20020919 More vulnerabilities (Re: Security side-effects of Word fields)
ISS X-Force Database: word-includetext-read-files (10008): Microsoft Word INCLUDETEXT field in shared documents can be used to read other files	Broken Link web.archive.org text/html Inactive Link Not Archived	 XF word-includetext-read-files(10008)
ISS X-Force Database: word-includepicture-read-files (10155): Microsoft Word INCLUDEPICTURE field in shared documents can be used to read other files	Broken Link web.archive.org text/html Inactive Link Not Archived	 XF word-includepicture-read-files(10155)
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.		

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Excel	2002	All	All	All
Application	Microsoft	Excel	2002	sp1	All	All
Application	Microsoft	Excel	2002	sp2	All	All
Application	Microsoft	Excel	2002	All	All	All
Application	Microsoft	Excel	2002	sp1	All	All
Application	Microsoft	Excel	2002	sp2	All	All
Application	Microsoft	Word	All	All	All	All
Application	Microsoft	Word	2000	All	All	All
Application	Microsoft	Word	2000	sp2	All	All

cpe:2.3:a:microsoft:word:*:*:*:*:mac_os_x:*:*:
cpe:2.3:a:microsoft:word:2000:*:*:*:*:*:
cpe:2.3:a:microsoft:word:2000:sp2:*:*:*:*:*:
cpe:2.3:a:microsoft:word:2000:sr1:*:*:*:*:*:
cpe:2.3:a:microsoft:word:2000:sr1a:*:*:*:*:*:
cpe:2.3:a:microsoft:word:2001:*:*:*:*:mac_os_x:*:*:
cpe:2.3:a:microsoft:word:2002:*:*:*:*:*:
cpe:2.3:a:microsoft:word:2002:sp1:*:*:*:*:*:
cpe:2.3:a:microsoft:word:2002:sp2:*:*:*:*:*:
cpe:2.3:a:microsoft:word:97:*:*:*:*:*:
cpe:2.3:a:microsoft:word:97:sr1:*:*:*:*:*:
cpe:2.3:a:microsoft:word:97:sr2:*:*:*:*:*:
cpe:2.3:a:microsoft:word:98:*:*:*:*:*:
cpe:2.3:a:microsoft:word:98:*:*:*:*:mac_os_x:*:*:
cpe:2.3:a:microsoft:word:98:*:*:ja:*:*:*:
cpe:2.3:a:microsoft:word:*:*:*:*:mac_os_x:*:*:
cpe:2.3:a:microsoft:word:2000:*:*:*:*:*:
cpe:2.3:a:microsoft:word:2000:sp2:*:*:*:*:*:
cpe:2.3:a:microsoft:word:2000:sr1:*:*:*:*:*:
cpe:2.3:a:microsoft:word:2000:sr1a:*:*:*:*:*:
cpe:2.3:a:microsoft:word:2001:*:*:*:*:mac_os_x:*:*:
cpe:2.3:a:microsoft:word:2002:*:*:*:*:*:
cpe:2.3:a:microsoft:word:2002:sp1:*:*:*:*:*:
cpe:2.3:a:microsoft:word:2002:sp2:*:*:*:*:*:
cpe:2.3:a:microsoft:word:97:*:*:*:*:*:
cpe:2.3:a:microsoft:word:97:sr1:*:*:*:*:*:
cpe:2.3:a:microsoft:word:97:sr2:*:*:*:*:*:
cpe:2.3:a:microsoft:word:98:*:*:*:*:*:
cpe:2.3:a:microsoft:word:98:*:*:*:*:mac_os_x:*:*:

cpe:2.3:a:microsoft:word:98:*:*:ja:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)